BUFFALO

レイヤー３インテリジェントスイッチ

BS-G3024MR

ハードウェア IP フィルタ設定ガイド

はじめにお読みください

● 本書について

本書は、本製品のハードウェア IP フィルタ機能に関する設定例およびコマンドリファレンスを記載したマニュアルです。本製品をご使用になる前には、はじめに「導入ガイド」をお読みください。また、コマンドラインインターフェースの詳細については、付属 CD に収録されている「リファレンスガイド」を参照してください。

● 「導入ガイド」および「リファレンスガイド」に記載の IP フィルタ機能について

ハードウェア IP フィルタ機能の実装に伴い、「導入ガイド」および「リファレンスガイド」に記載の IP フィルタが「ソフトウェア IP フィルタ」へと名称変更になりました。該当部分については、「ソフトウェア IP フィルタ」と読み替えてください。

導入ガイド　：P10、61、72、119
リファレンスガイド：P17、54、100

目次

1　機能概要 3

ハードウェア IP フィルタ機能について 3
設定の前に（初期設定） 3
ハードウェア IP フィルタ機能設定のながれ 4

2　設定例 5

サーバと、特定のネットワークとの通信を拒否する 5
特定の IP アドレスからの通信を許可する 7
TCP の片方向通信を許可する 9
特定アプリケーションの通信を許可する 11

3　コマンドリファレンス 13

ハードウェア IP フィルタ機能コマンド一覧 13
コマンド解説 14
　access-list 14
　no access-list 14
　permit / deny 14
　no permit / no deny 14
　ip access-list 16
　no ip access-list 16
　show access-list 17
　show access-list <list_name> 17
　show access-list status 18
IP プロトコル番号と TCP 制御コード 19

MEMO

1 機能概要

ハードウェア IP フィルタ機能の概要ついて説明します。

ハードウェア IP フィルタ機能について

ハードウェア IP フィルタ機能は、ポートの通過を許可(permit)または拒否(deny)する IP パケットの条件を定義したリストです。
作成したリストを特定のポートに適用することにより、IP アドレスやポート番号などの条件で、パケットの通過を許可または拒否することができます。
これにより、スループットを落とすことなく特定のパソコンのネットワークアクセスを制御し、セキュリティを向上させることができます。

メモ　ハードウェア IP フィルタ機能は、コマンドラインインターフェースからのみ設定できます。コマンドラインインターフェースについての詳細は、リファレンスガイド（付属 CD に収録）を参照してください。

設定の前に（初期設定）

ハードウェア IP フィルタ機能の設定をおこなう前に、設定をおこなうパソコンと本製品について、以下の操作をおこなってください。

- ネットワーク接続（Telnet）またはコンソール接続（ハイパーターミナルなど）
- 本製品へのログイン
- 本製品の IP アドレスの設定
- 特権モード（Privileged Exec）へのアクセス
- Configuration モードへの移行

メモ　各操作の詳細は、本製品付属の導入ガイドまたはリファレンスガイド(付属 CD に収録)を参照してください。

ハードウェア IP フィルタ機能設定のながれ

ハードウェア IP フィルタ機能設定のながれは、以下の通りです。

メモ　ハードウェア IP フィルタ機能は、コマンドでのみ設定できます。
（Web 画面上では設定できません）

1　条件リスト（Access Control List：ACL）の作成

↓

2　条件の定義（ルール）の作成

↓

3　条件を適用するインターフェースの選択

↓

4　条件の適用

↓

5　設定内容の保存

設定例：ポート 15 へ ACL 名「buffalo-test」を適用する場合

BS-G3024MR# configure	……	Config モードへ移行
BS-G3024MR(config)# access-list buffalo-test	……	**1** 条件リスト「buffalo-test」を作成
BS-G3024MR(config-access)# permit 192.168.10.0/24 any any any any any	……	**2** 条件の定義（ルール）を作成
BS-G3024MR(config-access)# deny 192.168.2.0/16 192.168.1.0/24 any any any any	……	条件の定義（ルール）を作成
BS-G3024MR(config-access)# deny any any any any any any	……	条件の定義（ルール）を作成
BS-G3024MR(config-access)# exit	……	Config モードに戻る
BS-G3024MR(config)# interface Ethernet 15	……	**3** 設定する対象ポートを指定
BS-G3024MR(config-if)# ip access-list buffalo-test inbound	……	**4** 上記ポートに「buffalo-test」を設定
BS-G3024MR(config-if)# exit	……	Config モードに戻る
BS-G3024MR(config)# system save	……	**5** 設定内容の保存
BS-G3024MR(config)# exit	……	特権モードに戻る

2 設定例

ハードウェア IP フィルタ機能の設定例を説明します。下記の設定例はあくまでも１例ですので、実際の環境にあわせて設定してください。

サーバと、特定のネットワークとの通信を拒否する

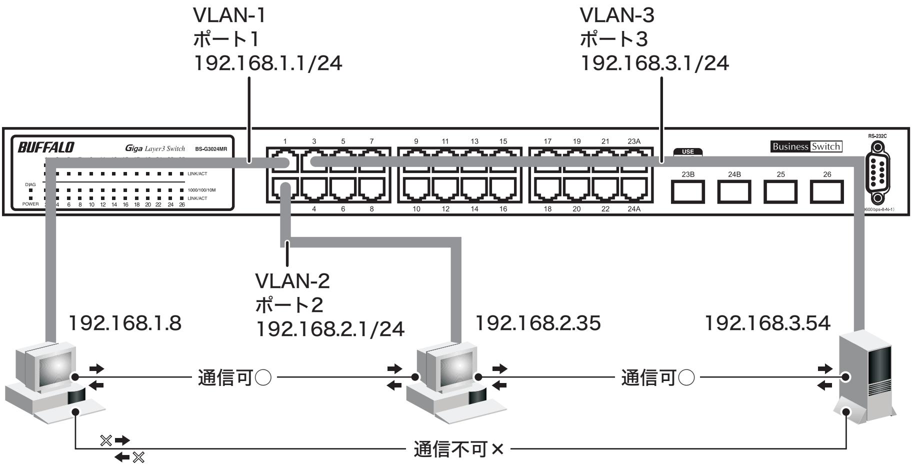
この例では、特定ポートに接続された VLAN と特定サーバとの通信を不可とする設定をおこないます。

使用環境（前提条件）

VLAN-1（ポート 1）と VLAN-2（ポート 2）と VLAN-3（ポート 3）が存在し、VLAN 間のルーティングが可能な環境とします。

フィルタリング条件

VLAN-1 のポート 1 に接続しているパソコンすべてから、VLAN-3 のサーバへ通信を拒否する設定にします。また、VLAN-3 のサーバから、VLAN-1 のネットワークへの通信を拒否する設定にします。



BS-G3024MR# configure terminal	……	Config モードへ移行
BS-G3024MR(config)# access-list test1	……	条件リスト「test1」を作成
BS-G3024MR(config-access)# deny 192.168.1.0/24 192.168.3.54/32	……	192.168.1.0/24 から 192.168.3.54/32 へのアクセスを拒否する
BS-G3024MR(config-access)# exit	……	Config モードに戻る
BS-G3024MR(config)# access-list test2	……	条件リスト「test2」を作成
BS-G3024MR(config-access)# deny 192.168.3.54/32 192.168.1.0/24	……	192.168.3.54/32 から 192.168.1.0/24 へのアクセスを拒否する
BS-G3024MR(config-access)# exit	……	Config モードに戻る
BS-G3024MR(config)# interface ethernet 1	……	ポート 1 の設定開始
BS-G3024MR(config-if)# ip access-list test1 inbound	……	「test1」を inbound として設定
BS-G3024MR(config-if)# exit	……	Config モードに戻る
BS-G3024MR(config)# interface ethernet 3	……	ポート 3 の設定開始
BS-G3024MR(config-if)# ip access-list test2 inbound	……	「test2」を inbound として設定
BS-G3024MR(config-if)# exit	……	Config モードに戻る
BS-G3024MR(config)# system save	……	設定内容の保存
BS-G3024MR(config)# exit	……	特権モードに戻る

特定の IP アドレスからの通信を許可する

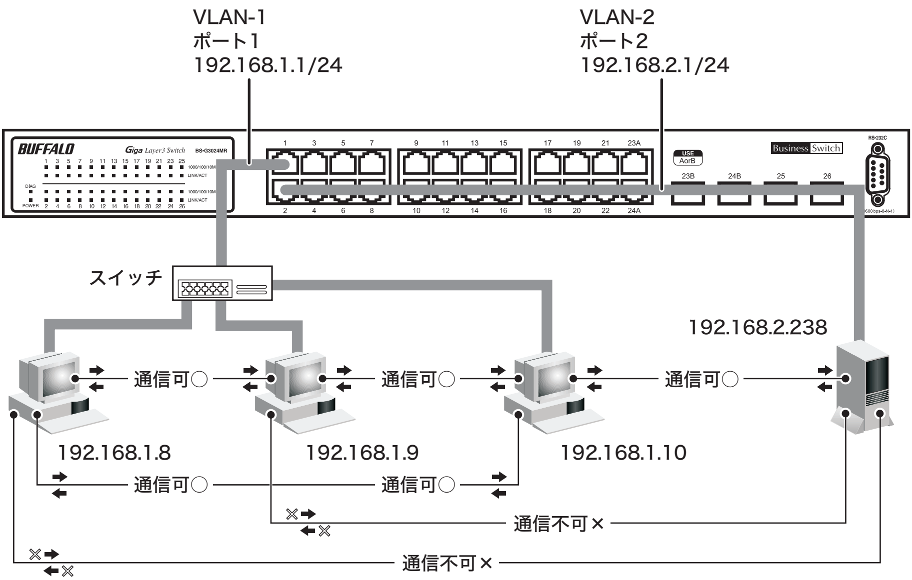
この例では、特定の IP アドレスをもったパソコンからのみ、特定の VLAN への通信を許可する設定をおこないます。

使用環境（前提条件）

VLAN-1（ポート 1）と VLAN-2（ポート 2）が存在し、VLAN 間のルーティングが可能な環境とします。

フィルタリング条件

VLAN-1 のポート 1 の配下にあるパソコン（192.168.1.10）からのみ、VLAN-2 のネットワークへの通信を許可する設定にします。また、VLAN-2 のポート 2 の配下にあるパソコンから、VLAN-1 のパソコン（192.168.1.10）以外への通信を拒否する設定にします。



BS-G3024MR# configure terminal	……	Config モードへ移行
BS-G3024MR(config)# access-list test1	……	条件リスト「test1」を作成
BS-G3024MR(config-access)# permit 192.168.1.10/32 192.168.2.0/24	……	192.168.1.10/32 から 192.168.2.0/24 への通信を許可する
BS-G3024MR(config-access)# deny any 192.168.2.0/24	……	上記条件以外で、宛先 IP アドレスが 192.168.2.0/24 への通信を拒否する
BS-G3024MR(config-access)# exit	……	Config モードに戻る
BS-G3024MR(config)# access-list test2	……	条件リスト「test2」を作成
BS-G3024MR(config-access)# permit 192.168.2.0/24 192.168.1.10/32	……	192.168.2.0/24 から 192.168.1.10/32 への通信を許可する
BS-G3024MR(config-access)# deny any 192.168.1.0/24	……	上記条件以外で、宛先 IP アドレスが 192.168.1.0/24 への通信を拒否する
BS-G3024MR(config-access)# exit	……	Config モードに戻る
BS-G3024MR(config)# interface ethernet 1	……	ポート 1 の設定開始
BS-G3024MR(config-if)# ip access-list test1 inbound	……	「test1」を inbound として設定
BS-G3024MR(config-if)# exit	……	Config モードに戻る
BS-G3024MR(config)# interface ethernet 2	……	ポート 2 の設定開始
BS-G3024MR(config-if)# ip access-list test2 inbound	……	「test2」を inbound として設定
BS-G3024MR(config-if)# exit	……	Config モードに戻る
BS-G3024MR(config)# system save	……	設定内容の保存
BS-G3024MR(config)# exit	……	特権モードに戻る

TCP の片方向通信を許可する

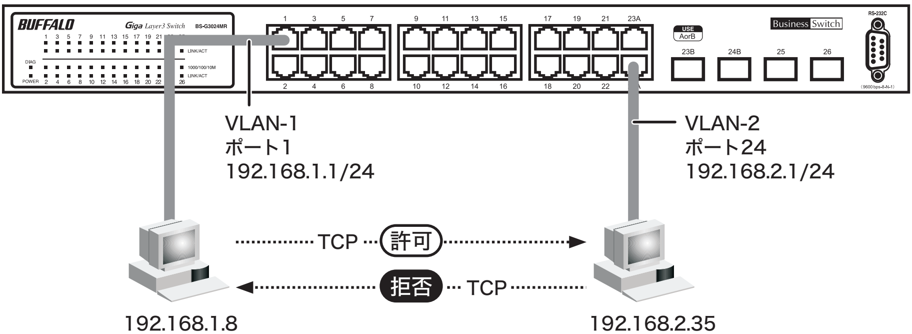
この例では、片側からのTCP通信を可能とし、もう片方からのTCP通信を不可とする設定をおこないます。

使用環境（前提条件）

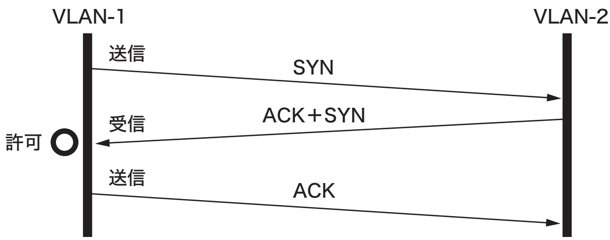
VLAN-1（ポート 1）と VLAN-2（ポート 24）が存在し、ルーティングが可能な環境とします。

フィルタリング条件

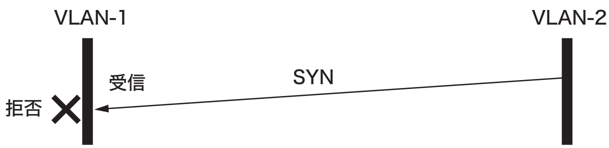
TCP プロトコル通信（プロトコル番号 6）のみを許可し、ポート 24 で受信する接続要求パケット（SYN パケット）は拒否します。
（ポート 1 側から開始するTCP通信を許可し、ポート 24側から開始するTCP通信を拒否します）



● ポート1側からの通信



● ポート24側からの通信



BS-G3024MR# configure terminal	……	Config モードへ移行
BS-G3024MR(config)# access-list test1	……	条件リスト「test1」を作成
BS-G3024MR(config-access)# permit any any 6	……	プロトコル番号 6（TCP）の通信を許可する
BS-G3024MR(config-access)# deny any any	……	上記条件以外の通信を拒否する
BS-G3024MR(config-access)# exit	……	Config モードに戻る
BS-G3024MR(config)# access-list test2	……	条件リスト「test2」を作成
BS-G3024MR(config-access)# deny any any 6 any any 2	……	プロトコル番号 6（TCP）かつ、TCP コントロールコード 2（SYN）を拒否する
BS-G3024MR(config-access)# permit any any 6	……	上記条件以外の TCP 通信を許可する
BS-G3024MR(config-access)# deny any any	……	上記条件以外の通信を拒否する
BS-G3024MR(config-access)# exit	……	Config モードに戻る
BS-G3024MR(config)# interface ethernet 1	……	ポート 1 の設定開始
BS-G3024MR(config-if)# ip access-list test1 inbound	……	「test1」を inbound として設定
BS-G3024MR(config-if)# exit	……	Config モードに戻る
BS-G3024MR(config)# interface ethernet 24	……	ポート 24 の設定開始
BS-G3024MR(config-if)# ip access-list test2 inbound	……	「test2」を inbound として設定
BS-G3024MR(config-if)# exit	……	Config モードに戻る
BS-G3024MR(config)# system save	……	設定内容の保存
BS-G3024MR(config)# exit	……	特権モードに戻る

特定アプリケーションの通信を許可する

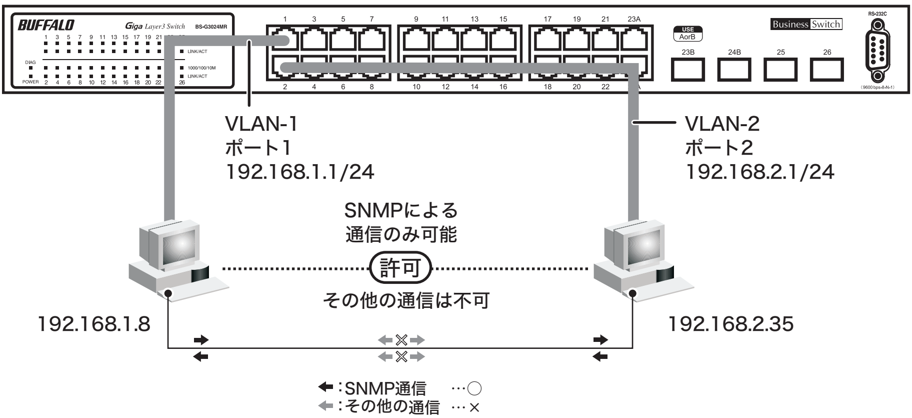
この例では、任意のポートに接続されたパソコン間で、特定のアプリケーションの通信のみ可能にする設定をおこないます。

使用環境（前提条件）

VLAN-1（ポート 1）と VLAN-2（ポート 2）が存在し、VLAN 間のルーティングが可能な環境とします。

フィルタリング条件

VLAN-1、2 間において、SNMP アプリケーション（UDP ポート番号 161）による通信のみを許可し、他の通信は拒否します。



`BS-G3024MR# configure terminal`	……	Config モードへ移行
`BS-G3024MR(config)# access-list test1`	……	条件リスト「test1」を作成
`BS-G3024MR(config-access)# permit any any 17 161 any`	……	プロトコル番号 17（UDP）かつ、送信元ポート番号が 161 の通信を許可する
`BS-G3024MR(config-access)# permit any any 17 any 161`	……	プロトコル番号 17（UDP）かつ、宛先ポート番号が 161 の通信を許可する
`BS-G3024MR(config-access)# deny any any`	……	上記条件以外の通信を拒否する
`BS-G3024MR(config-access)# exit`	……	Config モードに戻る
`BS-G3024MR(config)# interface ethernet 1`	……	ポート 1 の設定開始
`BS-G3024MR(config-if)# ip access-list test1 inbound`	……	「test1」を inbound として設定
`BS-G3024MR(config-if)# exit`	……	Config モードに戻る
`BS-G3024MR(config)# interface ethernet 2`	……	ポート 2 の設定開始
`BS-G3024MR(config-if)# ip access-list test1 inbound`	……	「test1」を inbound として設定
`BS-G3024MR(config-if)# exit`	……	Config モードに戻る
`BS-G3024MR(config)# system save`	……	設定内容の保存
`BS-G3024MR(config)# exit`	……	特権モードに戻る

3 コマンドリファレンス

ハードウェア IP フィルタ機能に関するコマンドについて説明します。

ハードウェア IP フィルタ機能コマンド一覧

ハードウェア IP フィルタ機能に関するコマンドは、以下の通りです。

コマンド	説明	ページ
access-list no access-list	条件リスト（ACL：アクセスコントロールリスト）を追加 / 削除します。	14 ページ
permit / deny no permit / no deny	フィルタのルール作成 / 削除をおこないます。permit を指定した場合は、対象のパケットを通過させます。deny を指定した場合は、対象パケットを破棄します。	14 ページ
ip access-list no ip access-list	条件リストをポートに適用 / 削除します。	16 ページ
show access-list	条件リストの情報を表示します。	17 ページ
show access-list <list_name>	指定した条件リストの情報を表示します。	17 ページ
show access-list status	条件リストのリソース情報を表示します。	18 ページ

コマンド解説

access-list
no access-list

条件リスト（ACL：アクセスコントロールリスト）を追加 / 削除します。

【コマンドの構文】

access-list <list_name>
no access-list <list_name>

【パラメータ】

<list_name>	条件リストの名前を、半角英数字、"-"（ハイフン）、"_"（アンダーバー）で 14 文字以内（スペースは不可）で指定します。

【デフォルト設定】

なし

【コマンドモード】

Global configuration

【コマンドの例】

```
BS-G3024MR# configure
BS-G3024MR(config)# access-list buffalo
BS-G3024MR(config-access)#
```

※条件リストは、最大 128 個まで作成できます。

permit / deny
no permit / no deny

フィルタのルール作成 / 削除をおこないます。
permit を指定した場合は、対象のパケットを通過させます。
deny を指定した場合は、対象パケットを破棄します。

【コマンドの構文】

permit <src_ip> <dst_ip> <protocol_number> <src_port> <dst_port> <tcp_control_code>
deny <src_ip> <dst_ip> <protocol_number> <src_port> <dst_port> <tcp_control_code>
no permit <src_ip> <dst_ip> <protocol_number> <src_port> <dst_port> <tcp_control_code>
no deny <src_ip> <dst_ip> <protocol_number> <src_port> <dst_port> <tcp_control_code>

【パラメータ】

<src_ip>	送信元 IP とネットマスクを指定します。 （例：192.168.1.10/32）
<dst_ip>	送信先 IP とネットマスクを指定します。 （例：192.168.2.20/25）
<protocol_number>	IP プロトコル番号（1 ～ 255）を指定します。 （例：ICMP 1、TCP 6、UDP 17）
<src_port>	TCP/UDP 送信元ポート番号（1 ～ 65535）を指定します。
<dst_port>	TCP/UDP 送信先ポート番号（1 ～ 65535）を指定します。
<tcp_control_code>	TCP 制御コード（FIN、SYN、RST、PSH、ACK、URG）を 1 ～ 63 で指定します。

【デフォルト設定】

なし

【コマンドモード】

ACL configuration

【コマンドの例】

```
BS-G3024MR# configure
BS-G3024MR(config)# access-list buffalo-test
BS-G3024MR(config-access)# permit 192.168.10.0/24 any any any any
any
BS-G3024MR(config-access)# deny 192.168.2.0/16 192.168.1.0/24 any
any any any
BS-G3024MR(config-access)# deny any any any any any any
BS-G3024MR(config-access)#
```

※ 各パラメータに any を指定することができます。any を指定した項目は評価されません。
※ <protocol_number>、<src_port>、<dst_port>、<tcp_contlol_code> は省略できます。省略した場合は、any を指定したのと同じになります。
例えば、deny 192.168.1.1/24 192.168.2.1/24 ルールは、deny 192.168.1.1/24 192.168.2.1/24 any any any any ルールと同等になります。
ただし、<src_port> を指定した場合、<dst_port> は省略できません。
※ <src_ip>、<dst_ip> にマルチキャストアドレスや 0.0.0.0、255.255.255.255 を指定することはできません。
※ <src_port>、<dst_port> は、<protocol_number> が 6（TCP）または 17（UDP）のときのみ指定できます。
※ <tcp_contlol_code> は、<protocol_number> が 6（TCP）のときのみ指定できます。
※ TCP の制御コードは、下位ビットからそれぞれ FIN、SYN、RST、PSH、ACK、URG です。例えば、SYN ビットのみセットするときは 2 を、ACK と SYN ビットをセットするときは 18 を指定します。
※ 1 つの条件リストの中に最大 16 個までルールを追加できます。
※ 1 つの条件リストの中に deny ルールが 1 つも存在しない場合、すべてのパケットが通過します。最低 1 つ deny ルールを指定してください。
※ deny any any any any any any ルールを指定する場合、一番最後に追加してください。
（途中の行で指定しても、実際は一番最後に実行されます）

※ 本製品自身が送信するパケット（RIP、SNMP トラップなど）は、outbound で deny ルールが設定されていても破棄されません。
※ ポートに条件リストが適用されている状態で、条件リストの内容を変更することはできません。

ip access-list
no ip access-list

条件リストをポートに適用 / 削除します。

【コマンドの構文】

ip access-list <list_name> <inbound | outbound>
no ip access-list <list_name> <inbound | outbound>

【パラメータ】

<list_name>	条件リストの名称（access-list コマンドで作成済みの名称）を指定します。	
<inbound | outbound>	inbound	：　入力パケットに適用します。
	outbound	：　出力パケットに適用します。

【デフォルト設定】

なし

【コマンドモード】

Interface configuration

【コマンドの例】

```
BS-G3024MR# configure
BS-G3024MR(config)# interface ethernet 15
BS-G3024MR(config-if)# ip access-list buffalo-list1 inbound
BS-G3024MR(config-if)# ip access-list buffalo-list2 outbound
BS-G3024MR(config-if)# exit
BS-G3024MR(config)#
```

※ permit ルールを含む条件リストを outbound に適用することはできません。
※ 1 つの物理ポートの 1 つの方向には、1 つの条件リストのみ適用してください。
※ 1 つの条件リストを inbound と outbound の両方に適用することはできません。
※ ポートに適用した条件リストを別の条件リストに適用し直す場合、先に適用した条件リストを no ip access-list コマンドで削除してから新しい条件リストを適用してください。

show access-list

条件リストの情報を表示します。

【コマンドの構文】

show access-list

【パラメータ】

なし

【デフォルト設定】

なし

【コマンドモード】

Privileged EXEC

【コマンドの例】

```
BS-G3024MR# show access-list
LIST1 LIST2 LIST3 LIST4..........
BS-G3024MR#
```

show access-list <list_name>

指定した条件リストの情報を表示します。

【コマンドの構文】

show access-list <list_name>

【パラメータ】

<list_name>　　条件リストの名称を指定します。

【デフォルト設定】

なし

【コマンドモード】

Privileged EXEC

【コマンドの例】

```
BS-G3024MR# show access-list LIST1
<ACL rule>
permit 192.168.10.0/24 any any any any any
deny any any any any any any

<Port binding>
Port3 - Inbound
BS-G3024MR#
```

show access-list status

条件リストのリソース情報を表示します。

【コマンドの構文】

show access-list status

【パラメータ】

なし

【デフォルト設定】

なし

【コマンドモード】

Privileged EXEC

【コマンドの例】

```
BS-G3024MR# show access-list status

Unused list table: 128
Used list table: 30
Total list table: 98

BS-G3024MR#
```

※ Unused list table は未使用の条件リスト数、Used list table は使用済みの条件リスト数、Total list table は本製品でサポートする条件リスト数を表します。

IP プロトコル番号と TCP 制御コード

主な IP プロトコル番号

IP プロトコル番号	プロトコル名
1	ICMP
2	IGMP
6	TCP
17	UDP

TCP 制御コード一覧

ビット	制御コード名
5	URG
4	ACK
3	PSH
2	RST
1	SYN
0	FIN

例：SYN のみセットされている制御コードを指定する場合「000010」なので 2、SYN と ACK のみセットされている制御コードを指定する場合「010010」なので 18、になります。

MEMO

BS-G3024MR ハードウェア IP フィルタ設定ガイド
2008 年 6 月 30 日　初版発行
発行 株式会社バッファロー